Below are several recent e-news items that may be of interest. One item that was discussed in our Aug 20 HIPAA Workgroup Meeting is the HIPAA Issues Website that is in testing. A document related to this is attached. We are continuing to enhance the Website and it will be released to production status in the next week or so. Also, please be sure to reference the list of meetings and conferences that is part of the HIPAA Workgroup Agenda.

A note of caution is given under the topic "certification". This may have some value.

Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

Many thanks to all who contributed to this information!!!
Have a great day!!!
Ken

Items included below are:
Shari Steele: "Privacy Rights: The Civil Perspective"
HHS' National Committee on Vital Health Statistics.
[hipaalive] AHIMA - HIPAA 'Minimum' Standards Need Strengthening
[hipaalive] PRIVACY: System Viewing Audits
[hipaalive] PRIVACY: Awareness and Training
[hipaalive] GENERAL: Data Collection Tools
[hipaalive] Certification
[hipaalive] GENERAL: Graham Leach vs. HIPAA
[hipaalive] SECURITY: Encryptions Requirements
[hipaalive] Privacy and Security Officer
[hipaalive] TCS: print image to EDI X12?

******************** Shari Steele: "Privacy Rights: The Civil Perspective" ****************************

>>> "Roberts, Bill" <Bill_Roberts@CalPERS.CA.GOV> 08/27/01 09:31AM >>>
Hello, Ken -

You may wish to consider the inclusion of the following event as a notification to interested parties:

Shari Steele LL.M, Executive Director of the Electronic Frontier Foundation will present: "Privacy Rights: The Civil Perspective" at the annual Information Security Conference at the Sacramento Convention Center on October 3rd. Invitation, agenda and biography are enclosed.

****************** HHS' National Committee on Vital Health Statistics.
****
FROM: Today's California Healthline on Aug. 24
Health Groups Outline Objections to HIPAA Privacy Rules for HHS Advisory Panel
Health industry leaders reiterated calls for revocation or revision of the HIPAA medical privacy rules on Tuesday, in testimony before an advisory panel of HHS' National Committee on Vital Health Statistics.
http://www.californiahealthline.org/members/basecontent.asp?contentid=43447&collectionid=3&contentarea=17971

********* [hipaalive] AHIMA - HIPAA 'Minimum' Standards Need Strengthening
****
*** This is HIPAAlive! From Phoenix Health Systems ***
This from California Site

AHIMA Official Says HIPAA 'Minimum' Standards Need Strengthening
08/23/2001

"Additional requirements" should be added to the Health Insurance Portability and Accountability Act's privacy provisions in order to keep patient health information from those who do not need access to all or part of it, a vice president of the American Health Information Management Association said yesterday. Testifying in Chicago before the Privacy and Confidentiality Subcommittee of HHS' National Committee of Vital and Health Statistics, Dan Rode said the following additions should be made to the HIPAA rule, which establishes the first comprehensive federal standards for medical privacy:

Providers should use "professional judgement" when releasing information and should only grant requests with sufficient "justification."

Certified health informational management professionals should handle all disclosures in order to "centralize" the process and to ensure that the release of information meets all legal requirements.

Those requesting protected medical information should be required to sign for the use of such information and verify it will be "limited to the minimum necessary for the stated purpose."

All released information should be destroyed once it has been used for its stated purpose.

The right for patients to "request restrictions" on the disclosure of their information should either be removed or become an option for providers and health plans to extend to patients. Rode said that this right is "contrary to the medical, ethical and legal obligations that require providers to maintain accurate and complete medical records."

Rode concluded that while the association supports the "important ... protections" given to patients under HIPAA, the additional standards are "needed" (AHIMA release, 8/22).

Allan Tobias, MD. JD
Healthcare Consulting & Law
(925) 935-5517
FAX (925) 932-2741
E-MAIL altoby@aol.com

****************** [hipaalive] PRIVACY: System Viewing Audits ****************************

*** This is HIPAAlive! From Phoenix Health Systems ***
The way we read the rule is:
1. Upon request from an individual, you must be able to show all instances where PHI was used OUTSIDE the realm of Treatment, Payment or Health Care operations.
2. Viewing a record in the normal course of business is WITHIN the realm of Treatment, Payment or Health Care Operations, so no list needs to be provided on demand.
3. The Security Rule mentions audit trails, but doesn't go into specific detail. We're taking that to mean that we may want to keep track of changes to data on a record-by -record basis (date, time and user who made the change). We might also log changes to certain specific fields. We're also looking into what it would take to change our security system so that all accesses (display or update) to Employee and VIP records are logged (since these are the records most likely to suffer privacy abuses).

That's just our read. Might be right, might not.
kweber@pinnaclesolns.com

** This is HIPAAlive! From Phoenix Health Systems ***
There are two separate HIPAA audit requirements.

The disclosure accounting requirement is specified in the privacy regulation at ? 164.528. It spells out the types of disclosures that are subject to accounting, which include everything except TPO, disclosures to subject individuals, disclosures to facility directories or persons involved in the subject individual's care, disclosures in correctional institutions, disclosures for national security or intelligence purposes, and disclosures that occur prior to the compliance date. This disclosure accounting requirement also specifies the mandatory content of each disclosure accounting record to include: the date of the disclosure, to whom the disclosure was made, a description of the information disclosed and the reason for the disclosure. At first glance, this doesn't seem like an audit requirement since you only have to produce these records if the subject individual requests them. But if you look at ? 164.528(d)(1), you see that you are required to maintain the disclosure accounting log whether you receive requests for disclosure accounting or not.

The other audit requirement is contained in the security rule at ? 142.308(c)(1)(ii). This audit log is not kept in order to report disclosures to subject individuals but rather for intrusion detection purposes. The regulation does not specify the specific information that must be included in these records, just that these audit controls are "mechanisms employed to record and examine system activity." Typical items recorded for intrusion detection purposes include logins/logouts, unsuccessful access attempts, audit policy changes, user privilege changes, etc.

It is unlikely that the audit capability built into the security components of operating systems, databases, network operating systems, etc. can be configured to provide the disclosure accounting log needed to comply with the privacy regulation requirement. But they should do an excellent job of meeting the security regulation requirement, since that is what they were designed to do. Recording disclosure accounting information will almost certainly be a manual process until some HIPAA-specific functionality is made available in commercial software offerings.

Bye for now -- Harry

Harry E. Smith, CISSP
Timberline Technologies LLC
Telephone: 303-717-0793
Email: Harry_E_Smith@TimberlineTechnologies.com

***************** [hipaalive] PRIVACY: Awareness and Training
****
*** This is HIPAAlive! From Phoenix Health Systems ***
Take a look at http://www.ehcca.com/presentations/HIPAAWest1/403.pdf
<http://www.ehcca.com/presentations/HIPAAWest1/403.pdf> . This was a presentation given at the HIPAA West Summit in San Francisco in June. You may find it a good starting place.
Kevin Johnston, RN
Regional Coordinator, Security & Privacy
PeaceHealth Oregon Region
**************** [hipaalive] GENERAL: Data Collection Tools
****
*** This is HIPAAlive! From Phoenix Health Systems ***
You might consider NCHICA's HIPAA EarlyView. $150 complete (cheaper for members). It only targets the Data Security rules, but other tools are in the pipeline. HIPAA EarlyView was developed by volunteer members from NCHICA, a non-profit

501(c)3 education association. www.nchica.org

Clyde Hewitt
Cii Associates, Inc.
Raleigh, NC

********************************** [hipaalive] Certification ***
*** This is HIPAAlive! From Phoenix Health Systems ***
And this vendor was selling what - Bridges? - Beach front property in Hawaii? - The cure for the common cold?

I've done enough laps around the sun to know that virtually nothing is IMPOSSIBLE, however, I'm having a hard time believing that HHS has authorized this, or any organization to certify HIPAA compliance. I'd be particularly interested in how they go about certifying compliance with the Security regs.

Ralph Mertz
Program Manager
Kindred Healthcare
(502)596-6499
ralph_mertz@kindredhealthcare.com

ORIGINAL FROM: Andrea.VanWanderham@healthsouth.com on 08/15/2001 12:32:07 PM
*** This is HIPAAlive! From Phoenix Health Systems ***
I just left a meeting where a vendor told me that they could certify HCO's as being HIPAA compliant. That they were authorized by HHS. Has anyone heard about this one before???
Thanks in advance,
Andrea

******************** [hipaalive] GENERAL: Graham Leach vs. HIPAA ******************************
*** This is HIPAAlive! From Phoenix Health Systems ***

Just want to echo Catherine's thoughts. Health insurance carriers are covered by GLB because there are viewed as "financial institutions". GLB is a Federal Law, but states can write their own version or adopt the Federal version. My health plan client had a state version and compliance was July 1, 2001 (already past), so the timing is different than HIPAA timing. However, we were able to still be efficient and avoid rework by cross-referencing HIPAA and GLB and analyzing the similar areas in tandem.
Miriam Paramore
miriam.paramore@hipaasurvival.com

502-895-2196

*** This is HIPAAlive! From Phoenix Health Systems ***
There may be some new resources, but as of a couple of months ago, there were no good comparative sources. We completed a combined HIPAA/GLB Privacy project for a client recently and had to develop our own cross-references and analytical tools. We were able to kill two birds with one stone on many of the requirements that are simliar (notice of information practices, disclosures, minimum necessary/reasonably necessary). Our presentation of this project can be found on the HIPAA Summit West site or the AFEHCT site. Please email me if you would like more information offline.

Regards,
Miriam Paramore
miriam.paramore@hipaasurvival.com
*********************** [hipaalive] SECURITY: Encryptions Requirements ************************
*** This is HIPAAlive! From Phoenix Health Systems ***
In this context, you are referring to DES which uses a 56-bit key (there are 64 bits but 8 are check bits).

Triple DES in majority of implementations have one of the following characteristic.
EDE/DED
1. Use 2 unique keys (56 + 56).
2. a) DES encrypt using key 1;
   b) DES decrypt results of 2. a) using key 2;
   c) DES encrypt results of 2. b) using key 1.
Note: if key 1 = key 2 this process is the same as DES.
To decrypt,
3. a) DES decrypt encrypted message from step 2 using key 1;
   b) DES encrypt results of 3. a) using key 2;
   c) DES decrypt results of 3. b) using key 1.

An alternative and similar method is EEE/DDD:
1. Use 2 unique keys (56 + 56).
2. a) DES encrypt using key 1;
   b) DES encrypt results of 2. a) using key 2;
   c) DES encrypt results of 2. b) using key 1.

To decrypt,
3. a) DES decrypt encrypted message from step 2 using key 1;
   b) DES decrypt results of 3. a) using key 2;
   c) DES decrypt results of 3. b) using key 1.

So if time is not an impediment, you might take your free 56-bit encryption (highly probable to DES) and apply the above process.

The Triple DES came about several years ago when the US
controlled export of algorithms having higher potential than
56 bits. Double DES only provides about 57 bits of
protection and if Key 1 = key 2 AND you use ED, then you
create unencrypted (asks for problems of implementation).

So some latency overhead (more/inefficient processing) versus
buying 3DES (more processing but also slightly more efficient).

I hope this helps a little.
Jack

*** This is HIPAAlive! From Phoenix Health Systems ***
Single DES (i.e. 56 bit) is currently being cracked in about 20 hours using
$100,000 worth of equipment. Many people consider this to be out of the
"acceptable risk" bounds. Triple DES is safe from everyone except possibly
the NSA.
Bye for now -- Harry
Harry E. Smith, CISSP
Timberline Technologies LLC
Telephone: 303-717-0793
Email: Harry_E_Smith@TimberlineTechnologies.com

*** This is HIPAAlive! From Phoenix Health Systems ***
You haven't missed anything.
If you need a standard, look at the HCFA Internet Security Policy where it
addresses "Acceptable Encryption Approaches".
www.hcfa.gov/security/isecplcy.htm
<http://www.hcfa.gov/security/isecplcy.htm>
It's dated 1998, but it will give you a good start.

*********************** [hipaalive] Privacy and Security Officer
****
*** This is HIPAAlive! From Phoenix Health Systems ***

I would have to agree with Nathan. We use a case study called "The Omega
Files" in our NCHICA HIPAA Security Lessons, taken from the real Omega
Engineering case several years ago. It highlights the risks of giving one
individual the keys to the entire castle. Here is a link to the CNN report:
http://www.cnn.com/2000/TECH/computing/06/27/omega.files.idg/

Clyde Hewitt
Cii Associates, Inc.
Raleigh, NC

***************************** [hipaalive] TCS: print image to EDI X12? ******************
*** This is HIPAAlive! From Phoenix Health Systems ***

You may want to review the work already completed by AFEHCT.
They have devoted much time and effort in a project called ASPIRE.
A summary of their findings for Professional and Institutional claims may be found at: http://www.afehct.org/aspire.asp.
Hope this helps.

Tom Drinkard
EDIT